==========
H I P A A L E R T -- Volume 4, Number 1 - January 21, 2003

>>From Phoenix Health Systems--HIPAA Knowledge--HIPAA Solutions<<
=>Healthcare IT Consulting & Outsourcing<=
==========
HIPAAlert is published monthly in support of the healthcare industry's efforts to work together towards HIPAA security and privacy. Direct subscribers total almost 20,000.

IF YOU LIKE HIPAAlert, YOU'LL LOVE HIPAAdvisory.com! -- Phoenix' "HIPAA Hub of the Web"
http://www.hipaadvisory.com
==========

Going to the HIMSS 2003 Conference in February?

STOP BY PHOENIX' BOOTH #815 -- and get a firsthand look at our HIPAA Privacy Policy Template Suite, and our new Small Provider Assessment and Planning Toolkit. Or, visit HIPAAdvisory.com to learn more: http://www.hipaadvisory.com

==========

T H I S I S S U E

==========

Behind on your HIPAA planning?

Phoenix Health Systems' Audio Conference
"11TH HOUR HIPAA: Meeting the Deadlines When You Haven't Started!"
presents the Rapid HIPAA Implementation Process

NEXT THURSDAY, JAN. 30, 2:00 - 3:00 PM EST

For more information or to sign up, visit our HIPAAstore:
http://www.hipaadvisory.com/ezcart/

==========

1 >> F R O M T H E E D I T O R S:

After three years of reporting on HIPAA and its dramatic regulatory fits and starts, it is of particular significance to this staff that the healthcare industry is nearing something of a

"HIPAAclimax" - the Privacy Rule compliance deadline is almost upon us. Further, (we are told, again) that the final Security Rule will be published within days.

What remains to be seen is whether or not healthcare providers, payers, clearinghouses and vendors are in sync. Phoenix Health Systems and HIMSS have just conducted our 12th quarterly national HIPAA progress survey; results are due out in our February issue. Unless the holidays were not as diverting as usual...unless the industry's sluggish 2002 compliance momentum has suddenly morphed into a burst of activity...unless smaller providers have finally "discovered" HIPAA...it seems fair to say that our Survey results will indicate more of a "HIPAAcrisis" than a "HIPAAclimax." Stay tuned...

In anticipation of the Security Rule finale, this issue features a special article by Steve Weil, CISSP, CISA, on the oft-referred-to, but infrequently-analyzed topic of the interrelationship between patient privacy and technical security measures. Eric Maiwald, CISSP, follows with an examination of the value of monitoring systems log files in a HIPAA-compliant environment. Finally, we return to patient privacy with Steve Fox and Rachel Wilson, Esqs, who offer a "real-world" examination of incidental uses and disclosures of protected health information("PHI").

D'Arcy Guerin Gue, Publisher
dgue@phoenixhealth.com

Bruce Hall,
Director of Internet Services
bhall@phoenixhealth.com

==========

2 >> H I P A A n e w s

*** Old Hard Drives Yield Data Bonanza ***

Security/privacy breaches continue to make the news...Two graduate students at the Massachusetts Institute of Technology (MIT) found more than 5,000 credit card numbers, medical reports, and detailed personal and corporate financial information on over 100 computer hard drives they bought for less than $1,000. Their findings, titled "Remembrance of Data Passed: A Study of Disk Sanitation," are being published in the January/February 2003 issue of IEEE Security and Privacy, a journal published by the IEEE Computer Society.

In a related story, a hard drive containing classified information may be missing from the Los Alamos National Laboratory. But, because of an inventory mistake, officials say they may never know. During an inventory of the lab's equipment last October, workers at the lab found a security bar code that was associated with an empty metal carrier that might have held a hard drive. The worker who put the bar code on the carrier admitted he had not looked inside at the time.

Read more: http://www.hipaadvisory.com/news/index.cfm#0121fcw

*** OCR Hiring Privacy Specialists for Nationwide Outreach ***

In an effort to allay health care industry confusion and anxiety as the April 14 compliance date nears, HHS' Office of Civil Rights (OCR), charged with overseeing HIPAA Privacy Rule compliance, is looking to hire Privacy Program Specialists to provide outreach and education. The Privacy Specialists, working out of 11 Regional Offices, will fan out across the country to increase awareness of covered entities' responsibilities and the public's rights under the Rule.

Read more: http://www.hipaadvisory.com/news/index.cfm#0115ocr

*** JCAHO Revises Business Associate Agreement with Hospitals ***

The Joint Commission on Accreditation of Health Care Organizations (JCAHO) has released its revised business associate agreement. Hospitals must sign the BA agreement as part of the application process for a JCAHO survey in order to be HIPAA-compliant. The American Hospital Association (AHA) says the revised agreement appropriately addresses hospital concerns.

Read JCAHO's revised BA agreement
(in Adobe Acrobat Portable Document Format):
http://www.hipaadvisory.com/action/privacy/JCAHOba.pdf

*** HHS to Hold Conferences on Privacy Rule ***

HHS will be holding four national one-day conferences, two in February and two in March, on the HIPAA Privacy Rule. The conferences are designed to provide an opportunity to hear from and interact with officials who developed the Privacy Rule and will be responsible for interpreting and enforcing the rule. The HHS Office for Civil Rights (OCR) will provide an expert faculty who will answer questions from attendees during question-and-answer sessions following their presentations.

Read more: http://www.hipaadvisory.com/news/index.cfm#0114ocr

==========

==========

3 >> H I P A A c t i o n: Feature Article

*** The HIPAA Security and Privacy Rules:
Intersections and Dependencies ***

By Steve Weil, CISSP, CISA

INTRODUCTION

Many organizations are falling into the trap of assuming that the HIPAA Privacy and Security Rules can be treated as independent regulations. The Privacy Rule, finalized and with a looming deadline of April 14, 2003 is the focus of many organizations while the Security Rule, not yet finalized, is being placed on the "back burner." Many organizations seem to have made a strategic decision to focus on the Security Rule after it's finalized and they finish meeting all the Privacy Rule requirements.

A careful examination of the two rules shows, however, that there are several important intersections between the two and that in order to fully comply with the Privacy Rule, organizations will need to understand and implement a number of the requirements outlined in the proposed Security Rule. This article examines these two areas in an effort to help organizations to streamline their HIPAA compliance efforts.

INTERSECTIONS

There are several areas where the Privacy and Security Rules requirements overlap or supplement each other. Understanding these intersections will enable organizations to more efficiently and effectively use organizational resources to comply with both rules.There are seven specific intersections:

1) Appropriate and reasonable safeguards:

Both rules require covered entities to take appropriate and reasonable measures to safeguard protected health information (PHI). More specifically, both require a covered entity (CE) to assess and define its own needs, select and implement protections appropriate for its own environment, and use a risk assessment process that strikes a balance between risk and remediation cost.

2) Mapping PHI dataflow:

To comply with both rules, CEs must understand and map their PHI data flow. In other words, they must know how and where PHI moves throughout their organization. Additionally, they must determine if PHI is being exchanged with outside entities such as business partners. Understanding the data flow is necessary if a CE is to choose and implement appropriate and reasonable PHI safeguards.

3) Protecting appropriate data:

The Privacy Rule's concept of a Legal Health Record (LHR), all individually-identifiable data, in any medium, collected and directly used in and/or documenting healthcare or health status, can be used to define the security responsibilities of a CE. The information that is included in the LHR is the data that must be appropriately protected by policies, procedures, and security technology. This means that some organizations will be able to save time and money by focusing efforts on their LHR rather than on all of the organization's data.

4) Access control:

The Security Rule states that CEs must use at least one of four types of access control (user based, context based, role based, or encryption) to limit access to PHI; the Privacy Rule clarifies this requirement. As discussed in its comment and response section, the final Privacy Rule states that role based access control is required. This means that CEs must create policies and procedures to identify (1) the types of persons within a CE that need access to PHI and (2) the specific PHI to which they require access. Specialized security technology and controls will be necessary to enforce these policies and procedures.

5) Third-party agreements:

Both rules require CEs to establish agreements between themselves and all other entities with whom PHI is shared in order to protect the data they exchange. This is to ensure that PHI is safeguarded at all times, even when it is no longer under the CE's direct control. CEs are also expected to periodically verify that the other entities are complying with the agreements. This principle is defined as a Business Associate Contract in the Privacy Rule and a Chain of Trust Partner Agreement in the Security Rule.

6) Accountability:

Both rules require that a specific person or group in a CE be assigned to make certain PHI is appropriately safeguarded. This promotes accountability, ensuring that a specific person or group can be held accountable for PHI use and disclosure rather than an "amorphous" organization. The principle is defined as Designating a Privacy Official in the Privacy Rule and Assigned Security Responsibility in the Security Rule.

7) Training and awareness:

Both rules require CEs to provide regular training to make certain all employees understand both the importance of protecting PHI and the means by which they must do so. Well-trained and aware employees are key to ensuring the protection of PHI.

PRIVACY RULE REQUIREMENTS DEPENDENT ON SECURITY RULE REQUIREMENTS

The Privacy Rule mandates that a CE safeguard all PHI that it holds, no matter the PHI's form. This includes PHI maintained or communicated on paper, electronically, or orally. In contrast, the proposed Security Rule focuses on what is required to safeguard PHI in electronic form. The Security Rule is based on information security best practices that dictate the policies, procedures and technology that is necessary to safeguard the confidentiality, integrity and availability of electronic PHI.

There are three specific areas where complying with Privacy Rule requirements will necessitate CEs implementing the security practices defined and required in the Security Rule. In these areas, the Privacy Rule principles provide a significant part of the basis for the Security Rule requirements, and the Security Rule requirements enforce the Privacy

Rule principles.

First, the Privacy Rule states, "A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart." To comply with this powerful and broad requirement, CEs will need to implement many of the requirements defined in the Security Rule, including taking steps to:

* Develop and implement a contingency plan so that the CE can effectively respond to disasters and ensure the availability of its PHI.

* Conduct regular audits of information system activity to ensure that PHI is being used or disclosed only by properly authenticated and authorized persons.

* Ensure that PHI has not been altered or destroyed in an unauthorized manner.

* Have a formal process for ending a person's employment or a user's access so that inappropriate access to PHI does not occur.

* Have consistent control of media containing PHI to ensure that unauthorized use or disclosure does not occur.

* Ensure that only properly authorized persons are allowed physical entry to a CE.

* Define the proper functions and location of workstations so that PHI is not inappropriately stored or viewed on a workstation.

* Develop and implement a well-defined change control process so that information system changes do not result in the inappropriate use or disclosure of PHI.

* Develop and implement security incident response procedures so that a CE can effectively detect, report, and respond to inappropriate use or disclosure of PHI. This includes procedures for handling security incidents at organizations with which a CE has exchanged PHI.

* Protect PHI sent across the Internet.

Second, the Privacy Rule states, "When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request."

To comply with this mandate, CEs will need to develop and implement security policies, procedures and technology based on the Security Rule requirements that (1) enforce appropriate access control and (2) audit the use and disclosure of PHI. Overall, they will need to implement a formal security policy and process that appropriately secures PHI during its entire lifecycle, from creation to disposal. These steps are required to ensure that CEs use or disclose PHI only on a need to know basis; this both safeguards PHI and provides the minimum amount of information necessary for authorized persons to perform their duties.

Third, the Privacy Rule states, "An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested." In the future, it is reasonable to expect an ever-increasing amount of PHI to be stored and released in electronic form. In order to meet this requirement, CEs will need to develop and implement security policies, procedures and technology based on the Security Rule requirements, that track and log the use and disclosure of PHI.

CONCLUSION

It is likely that the final Security Rule will result in even more intersections and dependencies with the Privacy Rule. As stated in the comment and response section of the Privacy Rule, "There should be no potential for conflict between the safeguards required by the Privacy Rule and the final Security Rule standards, for several reasons... . Second, in preparing the final Security Rule, the Department is working to ensure the Security Rule requirements for electronic information systems work hand in glove with any relevant requirements in the Privacy Rule..." Clearly, the lack of a final Security Rule does not relieve CEs of their responsibility for complying with the security implications of the Privacy Rule.

Understanding the Security Rule and appropriately implementing its measures will enable CEs to comply with specific requirements of the Privacy Rule. In addition to helping meet key Privacy Rule requirements, starting now on the Security Rule will give CEs a "head start" on Security Rule compliance and result in them following security best practices that their customers and business partners increasingly expect them to have.

Don't wait -- the time to start understanding and complying with the Security Rule is now.

Steven Weil, CISSP, CISA, is senior security consultant with Seitel Leeds & Associates, a full service consulting firm based in Seattle, WA. Mr. Weil specializes in the areas of security policy development, HIPAA compliance, disaster recovery planning and security assessments.

==========

4 >> H I P A A / SECURE: Security Q/A

*** Security Solutions: Key Technologies and Practices ***
>> Monitoring Log Files <<

By Eric Maiwald, CISSP

QUESTION: I understand that I should be monitoring the log files on my systems. What is the best way to do this?

ANSWER: Monitoring log files is indeed a good practice. Good information can be found in the event logs of servers, in firewall logs, and in intrusion detection system alerts. Unfortunately, the sheer amount of information from these sources can be overwhelming!

If your organization only has a small number of systems, it may be feasible for a member of the system administration or security staff to manually examine the log files of your systems. While this is a tedious job, it is possible for small amounts of information. Performed on a daily basis, the total amount of log entries that needs to be examined is small.

Unfortunately, it does not take many systems to create log files that will overwhelm someone who is looking at the log files manually. In this case, an automated tool is required. This tool can be as simple as a home-grown script that searches for certain types of log entries (error messages or denials for example) or it can be a more complex, commercial product.

Generally, what you should be looking for is something unusual. Seeing an internal system with a large number of failed login attempts or denials for file access may cause an investigation to find out why this is happening. Likewise, a firewall log that shows an internal system trying to make connections to some external connection at odd times of day may indicate a virus infection or a Trojan Horse program.

Do not expect the log file to tell you everything about the issue. You will likely have to do some additional investigation to find out exactly what is happening to cause the strange message.

Eric Maiwald, CISSP, is Chief Technology Officer of Fortrex Technologies, which provides information security management, and process and monitoring services for healthcare organizations and other industries.

==========

5 >> H I P A A / LAW: Legal Q/A

*** Incidental or Prohibited Use/Disclosure under HIPAA? ***

By Steve Fox & Rachel Wilson, Esqs.

With the April 14, 2003 compliance date looming larger by the minute, we thought it would be helpful to provide some concrete examples of how to apply the HIPAA Privacy Rule (the "Rule") in real-world situations. This month, we focus on incidental uses and disclosures of protected health information ("PHI").

INCIDENTAL USE AND DISCLOSURE

Incidental uses and disclosures of PHI are secondary uses or disclosures that occur as a by-product of a use or disclosure permitted under the Rule. Such uses and disclosures are permitted under the Rule so long as reasonable efforts have been undertaken, where applicable, to limit the PHI used or disclosed to the minimum amount necessary. The following scenarios, all of which are based on actual events experienced by one of the authors during the preceding week, highlight the importance of training and scrutinizing routine practices.

SCENARIO 1:

When patients are sent to the medical office laboratory for tests, the physician gives them a form indicating which lab tests have been ordered, and the patients are instructed to take the form to the lab. Upon arrival at the lab, the patient sees a table set up in front of a small sliding glass window, which is generally unattended. On the table is a sign-in sheet and a notice advising the patient to deposit the form into an open basket that sits adjacent to the sign-in sheet in the waiting room. The forms lie face-up in the basket, and include the patient's name, address, birth date, social security number and other demographic information.

PERMISSIBLE USE OR DISCLOSURE?

This practice is not HIPAA-compliant. Reasonable precautions have not been taken to minimize the chance of incidental disclosures and to limit the information disclosed to the minimum amount necessary. Although the disclosure described above is the incidental by-product of an otherwise permissible disclosure, precautions have not been taken to minimize the risk that PHI will be disclosed to other patients nor have there been any reasonable limitations placed on the amount of information disclosed. For example, if the purpose of the current procedure is simply for patients to sign-in to the lab area, that may be accomplishedwith the sign-in sheet alone, which requires only the patient's name. Eliminating the open basket would prevent disclosure of more sensitive PHI, including the specific tests that the doctor requested and all of the other patient demographic information. Moreover, the risk of incidental disclosure could be minimized by any number of reasonable alternatives, such as:

* relocating the basket inside the window, so that the forms would be in a location less visible and/or accessible to other patients;
* instructing patients to hand the form directly to a lab employee;
* placing the form in a folder or envelope before providing it to the patient; or
* asking patients to deposit the form in a mail slot in the wall, leading to a private area off limits to patients.

SCENARIO 2:

A psychiatrist is dining out with friends when she is paged by her answering service, with

an urgent message to call one of her patients. Having left her own cell phone in her car, the doctor uses her dinner companion's phone to return the patient's call. The borrowed phone automatically maintains a log of the outgoing telephone number.

PERMISSIBLE USE OR DISCLOSURE?

Without question, the preceding scenario involves the (inadvertent) disclosure of PHI. Under the Rule, a disclosure occurs whenever information is transferred, or access to the information is made available or divulged in any manner, to a third-party individual or entity outside of the covered entity. The patient's phone number constitutes PHI because it may easily be used to identify or contact the patient.

Although the disclosure described above may not be technically prohibited under the Rule, since it is not a disclosure to, or request by, a provider for treatment purposes, the minimum necessary rule is applicable. So, if there is a pay phone available to the psychiatrist or if it is possible or appropriate for the psychiatrist to wait and contact the patient from her home or office, she has an obligation to avail herself of such an option. Similarly, she could have used the borrowed phone to call her answering service and ask them to transfer her directly to the patient. In that case, only the answering service's telephone number would have been left on the phone's log, and no PHI would have been disclosed. (The appropriateness of calling the patient from a booth in a crowded restaurant will have to await a future column.)

SCENARIO 3:

During a routine blood test, a patient chats with the lab technician about a recent sporting event. The lab technician responds by telling an amusing anecdote concerning a well known sports figure who happened to have his blood test on the previous day.

PERMISSIBLE USE OR DISCLOSURE?

There is no justification under these circumstances for a staff member to discuss any aspect of one patient's care or treatment with another patient. This is not an inadvertent or incidental disclosure, but is purely the result of a lack of education and training on the part of the covered entity.

CONCLUSION

There is no expectation that covered entities will be able to protect PHI from any and all potential risk of inadvertent use or disclosure. Nor is the Rule intended to impede customary and necessary practices, such as using sign-in sheets, keeping patient folders outside of examining rooms or calling patients by name from the waiting room. Rather, HIPAA's goal is to insure that covered entities utilize reasonable safeguards, policies and procedures to insure that PHI will be protected, utilizing not less than a reasonable standard of care as defined by the Rule.

Read past HIPAA Legal Q/A articles:
http://www.hipaadvisory.com/action/LegalQA/archives.htm

Steve Fox, Esq., is a partner at the Washington, DC office of Pepper Hamilton LLP. This article was co-authored by Rachel H. Wilson, Esq., of Pepper Hamilton.
DISCLAIMER: This information is general in nature and should not be relied upon as legal advice.

==========

==========